ORIGINAL

DOC # 1

Approved: _____
NICOLE FRIEDLANDER/SARAH LAI/EUN YOUNG CHOI
Assistant United States Attorneys

Before: THE HONORABLE RONALD L. ELLIS
United States Magistrate Judge
Southern District of New York

15 MAG 250

15 MAG 2508

- - - - - - - - - - - - - - - - X

UNITED STATES OF AMERICA :

- v. - :

ANTHONY R. MURGIO, :

Defendant. :

- - - - - - - - - - - - - - - - X

SEALED COMPLAINT

Violations of 18 U.S.C §§ 371, 1956, 1960 and 2; 31 U.S.C. §§ 5318(g) and 5322(a)

COUNTY OF OFFENSE: NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

JOEL DECAPUA, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE
(Conspiracy to Operate an Unlicensed Money Transmitting Business)

1. From at least in or about April 2013 to at least in or about July 2015, in the Southern District of New York and elsewhere, ANTHONY R. MURGIO, the defendant, and others known and unknown, unlawfully, willfully and knowingly, did combine, conspire, confederate, and agree together and with each other to commit an offense against the United States, to wit, to violate 18 U.S.C. § 1960.

2. It was a part and an object of the conspiracy that ANTHONY R. MURGIO, the defendant, and others known and unknown, unlawfully, willfully and knowingly would and did conduct, control, manage, supervise, direct, and own all and part of an unlicensed money transmitting business, to wit, Coin.mx, d/b/a

"Collectables Club," d/b/a "Currency Enthusiasts" ("Coin.mx") in violation of Title 18, United States Code, Section 1960.

Overt Acts

3. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about April 30, 2013, ANTHONY R. MURGIO, the defendant, established an account at a particular financial institution ("Bank-1");

b. On or about October 17, 2013, MURGIO registered the domain name "Coin.mx" with a domain registrar;

c. Between at least in or about October 2013 and at least in or about February 2015, a co-conspirator not named as a defendant herein ("CC-1") exchanged emails and other electronic communications with MURGIO regarding Coin.mx;

d. On or about May 9, 2014, CC-1 agreed to join the board of a credit union in part to oversee a financial account through which Coin.mx processed customer transactions;

e. From in or about December 2013, through at least in or about November 2014, in an effort to promote Coin.mx and expand its customer base, MURGIO exchanged numerous emails with a company located in New York, New York.

(Title 18, United States Code, Section 371.)

COUNT TWO
(Operation of an Unlicensed Money Transmitting Business)

4. From at least in or about April 2013 to at least in or about July 2015, in the Southern District of New York and elsewhere, ANTHONY R. MURGIO, the defendant, willfully and knowingly did conduct, control, manage, supervise, direct, and own all or part of an unlicensed money transmitting business affecting interstate and foreign commerce, to wit, Coin.mx, an internet-based Bitcoin exchange business, which failed to comply with the money transmitting business registration requirements set forth in federal law and regulations.

(Title 18, United States Code, Sections 1960 and 2.)

COUNT THREE
(Money Laundering)

5. From at least in or about October 2013 to at least in or about July 2015, in the Southern District of New York and elsewhere, ANTHONY R. MURGIO, the defendant, in an offense involving and affecting interstate and foreign commerce, did transport, transmit, and transfer, and attempt to transport, transmit, and transfer a monetary instrument and funds from a place in the United States to and through a place outside the United States and to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, to wit, to promote the operation of the unlawful money transmitting business Coin.mx, in violation of Title 18, United States Code, Section 1960, MURGIO transferred hundreds of thousands of dollars from bank accounts within the United States to bank accounts outside of the United States, and caused others to transfer hundreds of thousands of dollars to bank accounts within the United States from bank accounts outside of the United States, including via certain wire transfers which cleared through New York, New York.

(Title 18, United States Code, Section 1956.)

COUNT FOUR
(Willful Failure to File a Suspicious Activity Report)

6. From at least in or about October 2013 to at least in or about July 2015, in the Southern District of New York and elsewhere, ANTHONY MURGIO, the defendant, willfully failed to report suspicious transactions relevant to possible violations of laws and regulations, as required by the Secretary of Treasury, to wit, MURGIO failed to file any Suspicious Activity Report as required by federal law and regulation with respect to numerous Bitcoin purchases conducted through Coin.mx by individuals who claimed they were being forced to make such purchases by cybercriminals who had gained remote control of their computers and were demanding "ransom" payments in Bitcoins to relinquish control of those computers.

(Title 31, United States Code, Sections 5318(g) and 5322(a); and Title 31, Code of Federal Regulations, Section 1022.320)

The bases for my knowledge and the foregoing charges are, in part, as follows:

7. I am a Special Agent with the FBI. I am currently assigned to the Computer Intrusion Squad of the New York Division of the FBI, and have received training in computer technology, computer fraud, intellectual property crimes, and white collar crimes. I am familiar with the facts and circumstances set forth below from my personal participation in the investigation, including my examination of reports and records, interviews I have conducted, and conversations with other law enforcement officers and other individuals. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, unless noted otherwise.

OVERVIEW

8. Since at least late 2013, ANTHONY R. MURGIO, the defendant, and his co-conspirators have knowingly operated Coin.mx, a Bitcoin exchange service, in violation of federal anti-money laundering ("AML") laws and regulations, including those requiring money services businesses like Coin.mx to meet registration and reporting requirements set forth by the United States Treasury Department.

9. As set forth below, through Coin.mx, MURGIO and his co-conspirators enabled their customers to exchange cash for Bitcoins, charging a fee for their service. In doing so, they knowingly exchanged cash for people whom they believed may be engaging in criminal activity, as set forth below. MURGIO and his co-conspirators have also knowingly exchanged cash for Bitcoins for victims of "ransomware" attacks, that is, cyberattacks in which criminals electronically block access to a victim's computer system until a sum of "ransom" money, typically in Bitcoins, is paid to them. In doing so, MURGIO and his co-conspirators knowingly enabled the criminals responsible for those attacks to receive the proceeds of their crimes, yet in violation of federal anti-money laundering laws, MURGIO never filed any suspicious activity reports regarding any of the transactions. In total, between approximately October 2013 and January 2015, Coin.mx exchanged at least $1.8 million for Bitcoins on behalf of tens of thousands of customers.

10. ANTHONY R. MURGIO, the defendant, and his co-conspirators engaged in substantial efforts to evade detection

of their scheme by operating through a phony front-company, "Collectables Club," and maintaining corresponding phony "Collectables Club" websites. In doing so, they sought to trick the major financial institutions through which they operated into believing their unlawful Bitcoin exchange business was simply a members-only association of individuals who discussed, bought, and sold collectable items, such as sports memorabilia. More recently, in an effort to evade potential scrutiny from these institutions and others, MURGIO and his co-conspirators acquired a federal credit union (the "Credit Union"), installed CC-1 and other co-conspirators on the Credit Union's Board of Directors, and transferred Coin.mx's banking operations to the Credit Union, which they operated, at least until early 2015, as a captive bank for their unlawful business.

BACKGROUND ON BITCOINS, THE REGULATION OF BITCOIN EXCHANGERS, and COIN.MX's FAILURE TO REGISTER WITH THE U.S. TREASURY DEPARTMENT

11. Based on my experience and participation in this investigation, I am aware of the following:

a. Bitcoins are an anonymous, decentralized form of electronic currency that exist entirely on the Internet and not in any physical form. Bitcoins are not illegal in and of themselves and have known legitimate uses. However, given the ease with which they can be used to move money anonymously, Bitcoins are also known to be used to facilitate illicit transactions and for money laundering purposes.

b. In order to acquire Bitcoins in the first instance, a user typically must purchase them from a Bitcoin "exchanger." Typically, in exchange for a fee, Bitcoin exchangers accept payments of currency in some conventional form (cash, wire transfer, etc.) and exchange the money for a corresponding amount of Bitcoins (based on a fluctuating exchange rate); similarly, they typically exchange Bitcoins for conventional currency. Once a user acquires Bitcoins from an exchanger, the Bitcoins are kept in an electronic "wallet" associated with a Bitcoin "address," designated by a complex string of letters and numbers. (The "address" is analogous to the account number for a bank account, while the "wallet" is analogous to a bank safe where the money in the account is physically stored.) Once a Bitcoin user funds his wallet, the user can use Bitcoins in the wallet to conduct financial transactions by transferring Bitcoins over the Internet from his Bitcoin address to the Bitcoin address of another user.

12. Based on my training and experience, I know the following about regulation of Bitcoin exchangers:

a. Exchangers of virtual currency, including Bitcoin exchangers, are considered money transmitters under federal law and are subject to federal AML regulations if they do substantial business in the United States. See 31 C.F.R. § 1010.100(ff)(5); see also Department of the Treasury Financial Crimes Enforcement Network, Guidance on the Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, March 18, 2013, FIN-2013-G001, available at http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

b. Specifically, federal regulations require a virtual currency exchanger to register with the Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") as a money services business and to develop and maintain an effective AML program. See 31 C.F.R. §§ 1022.210, 1022.380.

c. Maintaining an effective AML program requires filing Suspicious Activity Reports with FinCEN when appropriate, including reporting substantial transactions or patterns of transactions involving the use of the money services business to facilitate criminal activity. See 31 C.F.R. § 1022.320.

13. In or about July 2015, I searched a United States Treasury Department database containing the names of money services businesses lawfully registered to do business in the United States. From that search, I know that Coin.mx, "Collectables Club" and "Currency Enthusiasts" are not registered, and have never been registered, as a money services business with the United States Treasury Department. In addition, I have also searched that database for the surname "Murgio" and learned that no one with that surname has registered a money services business.

THE DEFENDANT'S DESIGN OF COIN.MX AS AN ILLEGAL BITCOIN EXCHANGE BUSINESS

14. I have reviewed emails and "chats" (another form of electronic communication) obtained pursuant to a search warrant authorized in this investigation for an email account registered in the name of "Anthony Murgio" ("MURGIO's Email Account"). I believe MURGIO's Email Account to be an email account of ANTHONY MURGIO, the defendant, for many reasons, including because the

user of the account identifies himself as MURGIO, is referred to by others as MURGIO (including with reference to MURGIO's education and employment history, with which I am familiar based on this investigation), and provides others with a copy of his driver's license, which based on my review matches that registered to MURGIO with the Florida Department of Motor Vehicles. From this review, I learned, in substance and in part, that:

a. Beginning in or about 2013, with various individuals, MURGIO discussed his plan to develop an internet-based Bitcoin exchange, sought funding for this new business, and thereafter explained that he had obtained funding to develop it. MURGIO also recruited managers and employees for his new Bitcoin exchange, including CC-1, as set forth below. Among other things, these communications reveal that MURGIO and his financial backers recognized from the outset that MURGIO intended to operate an illegal business. For example:

i. On or about September 30, 2013, MURGIO described his new business to an individual from whom he sought to obtain funding, explaining that it would be "for buying and selling" Bitcoins, "like a transmitter service."[1] Later that day, the individual explained that he would not risk investing in MURGIO's business because, while "I like BTC [Bitcoin]. . . I don't want to lose investment to the gov[ernment]. . . [It] would sting to [*sic*] bad if something happened."

ii. On or about October 14, 2013, MURGIO told another individual that while he had obtained a funding commitment from certain overseas investors, those investors "don't think the U.S. will like it, and they would not sleep if something would happen to me."[2]

---

[1] MURGIO described his business on numerous other occasions as a Bitcoin exchange business, including with reference to his understanding that U.S. law required it to be licensed. For example, in April 2014, in communicating with a particular overseas business, MURGIO described Coin.mx as "a digital money/bitcoin exchange" that was "interested in offering margin trading as well as having the ability to transfer money in and out of our members banks accounts [*sic*]. In the US the licenses would be a broker dealer and money transmitting."

[2] In January 2015, in an email in which he sought to convince a particular payment processor to do business with Coin.mx, MURGIO

b. In or about late September 2013, MURGIO recruited CC-1 to manage the development of a computer programming platform to support MURGIO's new Bitcoin-exchange business. For example, on or about October 17, 2013, MURGIO told CC-1 that "Coin.mx is going to be the brand," and that "it's mine now. . . and yours." MURGIO anticipated that Coin.mx would exchange "every currency and every digital currency," envisioning it as "a worldwide payment system with immediate funds availability." For his part, CC-1 expressed that he hoped to be "the founding father and the architect" of the Coin.mx electronic platform.

c. In exchange for payments, CC-1 agreed to, and did, become the "architect" of the Coin.mx electronic platform. For example, in certain of the communications:

i. CC-1 discussed his plan to rent, and his actual rental of, computer servers in the United States and abroad through which Coin.mx would and (based on my review of other evidence obtained in this investigation) did operate;

ii. CC-1 discussed his design of requisite programming specifications for the Coin.mx electronic exchange platform;

iii. Beginning in or about November 2013, MURGIO and CC-1 discussed hiring computer programming contractors whom CC-1 recommended to assist them in developing the Coin.mx platform, and whom CC-1 would and did manage and communicate with in order to develop that platform; and

---

suggested that he had "authority" to do business without a license because Coin.mx was a so-called "private member association," and that he notified unspecified federal and state authorities of the operation of his business "by certified mail." Contrary to this claim that MURGIO believed he had authority to run an unlicensed Bitcoin exchange, substantial evidence shows that MURGIO knowingly operated an unlawful business, including, as set forth herein, MURGIO and CC-1's various references to the unlawful nature of their business, MURGIO's lies to Bank-1 and Bank-2 about the nature of his business, and MURGIO and CC-1's creation of a phony front-company "Collectables Club" website to create the false appearance that they were operating a collectables trading association instead of an illegal Bitcoin exchange.

iv. After Coin.mx began operating in or about November 2013, CC-1 communicated regularly with MURGIO about maintaining, and resolving issues associated with, the programming operations of Coin.mx, and CC-1 and MURGIO continued to discuss potential changes to Coin.mx's computer programming infrastructure. For example, on or about February 1, 2014, CC-1 emailed MURGIO, for discussion, a diagram showing the Coin.mx technical infrastructure for a "Regular User" and an "Advanced Trader."

d. Like MURGIO, CC-1 recognized that Coin.mx was operating illegally. In addition, MURGIO and CC-1 recognized that their customers could be using Coin.mx's services to facilitate or launder the proceeds of criminal activity, and were excited by this prospect because, in their view, it represented the possibility of additional business for Coin.mx. For example:

i. On October 25, 2013, in discussing the development of Coin.mx, CC-1 complained that "the challenge" is that the "U.S. is not allowing funding for its own citizens," which, based on my experience and participation in this investigation, appears to be a reference to the fact that Coin.mx was operating in violation of federal law.

ii. In or about late 2013, CC-1 and MURGIO discussed configuring the Coin.mx programming infrastructure to keep a particular major Internet search engine from learning that Coin.mx was operating through multiple connected sites. Based on the evidence set forth below regarding the phony "Collectables Club" websites, I believe this is a reference to avoiding detection of the fact that the Collectables Club websites were phony front-companies for Coin.mx.

iii. On or about November 14, 2013, in a series of chats, CC-1 proposed that Coin.mx begin offering exchange services through Russia-based payment processors because "then a lot of [R]ussians can buy!!. . . and wash money as well." In response, MURGIO stated, in sum, that Coin.mx was already doing business with one or more such processors, in reply to which CC-1 wrote, "wow. . . how cool is that." Based on my training, experience, and participation in this investigation, I believe that in suggesting that Coin.mx enter into certain business arrangements that would encourage individuals in Russia to "wash money" through Coin.mx, CC-1 was expressing his hope that such arrangements would lead to Russia-based criminals using Coin.mx to launder the proceeds of their crimes.

e. While CC-1 supervised the computer programming functions of Coin.mx, MURGIO maintained financial and operational control of the company, including through his beneficial ownership and control of the company's financial accounts (aspects of which MURGIO discussed and directed through these emails and chats, and as further set forth below regarding MURGIO's control of Coin.mx's bank accounts), and through his oversight and control of the day-to-day management of the business, as reflected in numerous communications through which MURGIO recruited and hired employees, answered employees' questions about operating the Bitcoin exchange, and answered certain Bitcoin exchange customers' questions directly.

THE COIN.MX WEBSITE AND THE UNDERCOVER COIN.MX PURCHASES

15. From speaking with another federal agent involved in this investigation ("Agent-1"), I learned that on multiple occasions between approximately late 2014 and July 2015, Agent-1 visited the website www.coin.mx (the "Coin.mx Website," last visited July 16, 2015). According to the Coin.mx Website, Coin.mx was an "international . . . exchange that allows you to securely buy, use, and accept bitcoin and other digital currencies," and that accepts "CASH, WIRE & BANK DIRECT" as well as "ALL CREDIT CARDS." The website further claimed that Coin.mx "is open to 'anyone'" and that, as of in or about October 2014, Coin.mx had over "70,000 members!"

16. From reviewing records of an internet domain registrar (the "Domain Registrar") for the domain name "coin.mx," I learned that on or about October 17, 2013, an individual purporting to be named "Anthony Murgio" with a certain address in Florida (the "Florida Address") registered the internet domain name "coin.mx" using MURGIO's Email Account. The Florida Address is the same as the address for ANTHONY R. MURGIO, the defendant, on file with the Florida Department of Motor Vehicles. Accordingly, I believe that MURGIO registered the domain name "coin.mx" used by the Coin.mx Website.

17. From speaking with Agent-1, I have learned, in substance and in part, that in or about November 2014, acting in an undercover capacity in New York, New York, Agent-1 attempted to exchange U.S. dollars for Bitcoins through the Coin.mx Website, in the process of which he was asked through the website to sign a "Collectables Club Membership Agreement." According to the agreement, which I have reviewed, "Collectables Club" members "seek to help each other achieve information and

education pertaining to collection and trading of memorabilia." After Agent-1 agreed electronically through the Coin.mx Website to abide by that agreement, Coin.mx enabled Agent-1 to exchange U.S. dollars for Bitcoins through the Coin.mx Website, which Agent-1 subsequently did, as directed through the Coin.mx Website, in a successful undercover transaction. Several days later, through the Coin.mx Website, Agent-1 exchanged a portion of those Bitcoins back to U.S. dollars, which he successfully sent via wire transfer to, and then withdrew from, an undercover bank account. For each of these exchange transactions, Coin.mx charged Agent-1 a fee.

18. From speaking with Agent-1, I learned that in or about January 2015, Agent-1 again successfully exchanged U.S. dollars for Bitcoins through the Coin.mx Website. In addition, in or about July 2015, through the Coin.mx website, Agent-1 accessed Agent-1's Coin.mx account, and observed that it appeared to be functioning.

THE DEFENDANT'S EFFORTS TO EVADE DETECTION OF HIS SCHEME THROUGH THE PHONY "COLLECTABLES CLUB" FRONT-COMPANY

19. From reviewing bank and other records obtained in this investigation, I have learned that ANTHONY R. MURGIO, the defendant, and CC-1 attempted to evade detection of their unlawful Bitcoin exchange business by operating through a phony front-company, "Collectables Club," for which MURGIO maintained bank accounts and CC-1 maintained phony websites. These records further reveal that MURGIO has transferred hundreds of thousands of dollars between bank accounts in the United States and bank accounts overseas for the purpose of promoting his illegal Bitcoin exchange business.

20. From reviewing records of the Florida Department of State, Division of Corporations, I learned that ANTHONY R. MURGIO, the defendant, registered "Collectables Club" as a "doing business as" name with the State of Florida on or about July 15, 2013.

21. From reviewing bank records obtained in this investigation, I learned the following:

a. In or about August and October 2013, respectively, ANTHONY MURGIO, the defendant, opened bank accounts, on which he was the sole signatory, at Bank-1 and

another major U.S. financial institution ("Bank-2"),[3] each in the name "Collectables Club" (collectively, the "Bank-1 and -2 Collectables Club Accounts"), which in each case MURGIO claimed was a members-only association of collectables trading enthusiasts. For example, Bank-2 records reflect that in opening the Bank-2 Collectables Club Account, MURGIO informed Bank-2 that he was the founder and President of Collectables Club, which existed "to discuss various collectible items, items such as cars, coins, stamps, sports memorabilia, music instruments, etc.," and to exchange advice "on memorabilia trading, buying, selling, and information on events and meetings across the United States." Further, in terms of the purpose for which he would use the account, MURGIO told Bank-2 that "a small fee is charged for joining the club which is used to pay for meetings or retreat[s] the club would have on an annual basis. . . this account is use[d] to collect the membership dues and pay for gatherings."

b. In truth and in fact, MURGIO, CC-1, and their co-conspirators used the Bank-1 and -2 Collectables Club Accounts solely to operate Coin.mx. Specifically, between approximately September 2013 and mid-2014, through these accounts, MURGIO, CC-1 and their co-conspirators exchanged well over $1 million for Bitcoins on behalf of Coin.mx customers. In particular, among other things, the Bank-1 and -2 Collectables Club Account records show thousands of incoming deposits in varying amounts from individuals, some of whom, in wire transfer instructions, noted that their payment was "for Bitcoins." Similarly, the records show numerous payments to entities which I know, based on my training and experience, sell Bitcoins in exchange for U.S. dollars and other currency.

c. From the Bank-1 and -2 Collectables Club Accounts, MURGIO transferred hundreds of thousands of dollars in total to bank accounts in Cyprus, Hong Kong, and Eastern Europe in the names of one or more entities including, according to the records, as payment for "programming" and other services.[4]

---

[3] The Bank-2 records reflect that MURGIO opened and operated more than one such account at Bank-2. For ease of reference, these accounts are referred to collectively herein as the "Bank-2 Collectables Club Account."

[4] Further, communications in the MURGIO Email Account reflect that one or more of these accounts were owned by or for the benefit of Coin.mx and/or others working to operate the Coin.mx business. Specifically, in or about January 2014, an employee of Coin.mx asked MURGIO, in response to a customer's question,

MURGIO also received hundreds of thousands of dollars in total into the Bank-1 and -2 Collectables Club Accounts from bank accounts in Cyprus and the British Virgin Islands in the names of other entities. In addition to using money received into these accounts to exchange U.S. dollars for Bitcoins, as set forth above, MURGIO used the money to pay the operating expenses of Coin.mx. For example, the records show numerous periodic payments to individuals who I have learned, from my review of the MURGIO Email Account, were employees of Coin.mx.

22. In addition to the fact that ANTHONY R. MURGIO, the defendant, caused the Bank-1 and -2 Collectables Club Accounts to engage in the overseas transfers set forth above, emails in the MURGIO Email Account reflect that MURGIO directed certain of those transfers specifically in an effort to evade detection of his unlawful scheme. For example, by email dated November 28, 2013, a particular customer ("Customer-1") informed MURGIO that he was wiring $100,000 to the Bank-1 Collectables Club Account. In response, MURGIO wrote, "can you see if you can put a stop to it? . . . You may wire 20k to [Bank-1], it will be credited immediately. The rest must go to bulgaria please. We hope you understand the concerns. If the US was not so damn screwed up about this stuff, we wouldn't have to deal with this." Based on my training and experience, and my participation in this investigation, I believe that in providing these instructions, MURGIO demonstrated concern that due to its substantial size, a wire transfer of $100,000 could cause Bank-1 to scrutinize the transaction more closely, and thereby to discover that MURGIO was using the Collectables Club Account to operate an unlicensed Bitcoin exchange, and not a small collectables trading association, as MURGIO had falsely represented to Bank-1.

23. The MURGIO Email Account contains additional evidence that ANTHONY MURGIO, the defendant, sought to avoid detection of his unlawful scheme. For example, based on MURGIO Email Account communications that I have reviewed, in or about November 26, 2013, Customer-1 indicated that, in order to purchase thousands of dollars worth of Bitcoins, Customer-1 intended to instruct Customer-1's bank to wire money to Bank-1 for the benefit of "Collectables Club P.M.A.," which had the "nickname" of

---

whether a wire transfer into the customer's account from a particular entity's bank account was a wire "from us?" MURGIO responded, "yes." The Bank-1 and -2 Collectables Club Account records reflect wires of tens of thousands of dollars from and to bank accounts in the name of this particular entity located in Cyprus and the British Virgin Islands.

"Coin.mx." MURGIO replied, "I would **not** put coin.mx in there. Put Collectpma.com" (emphasis in original). In doing so, I believe, based on my training, experience, and participation in this investigation, that MURGIO demonstrated his knowledge that Bank-1 did not know that the Bank-1 Collectables Club Account was being used to operate MURGIO's illegal Coin.mx business, as well his intent to prevent Bank-1 from learning that fact.

24. I have learned that in a further effort to trick financial institutions and others into believing they were operating a collectables trading association, instead of an unlawful Bitcoin exchange business, ANTHONY R. MURGIO, the defendant, and CC-1 maintained phony "Collectables Club" websites. For example:

a. From reviewing the MURGIO Email Account, I learned that in or about April 2014, MURGIO referred a representative of Bank-1 to the website "http://collectpma.com" "so you can have a look at how everything works and the items that are available." In or about June 2015, I visited that website (the "Collectables Club Website") and observed that it stated prominently that it was the website of "Collectables Club," purportedly a members-only club that enables members to "buy and sell" antiques, "sports cards and memorabilia," "coins and currency," and other items through an online auction process. The website further claimed that the "Association" made money by charging 15 percent of the value of the transactions conducted through it, and contained purported links enabling website visitors to sign up with, and become members of, Collectables Club. However, at that time, after I completed and electronically submitted the purported online Collectables Club membership form, the website displayed an error message, and I was unable to become a member. Further, at that time, I viewed the images and product descriptions of certain items purportedly offered for sale on the Collectables Club Website, and observed that they were identical to items offered for sale on certain other online auction websites for which bidding had closed in or about late 2014. Based on my training, experience, and participation in this investigation, I believe MURGIO and his co-conspirators created this website, using photographs of items offered for sale on actual auction websites in the past, to create the false appearance to Bank-1 that MURGIO was operating a legitimate collectables trading association, instead of an illegal Bitcoin exchange.

b. I have reviewed emails obtained pursuant to a search warrant authorized in this investigation for an email

account registered in the name of CC-1 ("CC-1's Email Account"). I believe CC-1's Email Account to be an email account used by CC-1 for many reasons, including because the user of the account identifies himself by CC-1's name, and is referred to by others, including MURGIO, as CC-1 (including with reference to CC-1's employment history, with which I am familiar based on this investigation). From these emails, I learned, among other things, that CC-1 was tasked by MURGIO with maintaining the phony Collectables Club Websites in furtherance of the unlawful Coin.mx business, and that CC-1 did, in fact, maintain those websites, including by making changes to the websites at MURGIO's direction.

MURGIO'S FAILURE TO FILE A SAR REGARDING HIS PROCESSING OF RANSOM PAYMENTS FOR CYBERCRIMINALS

25. I have reviewed a report that a particular business (the "Victim") submitted to the FBI on or about August 15, 2014, spoken with another agent who interviewed a representative of the Victim (the "Victim's Representative"), and examined bank records for the Bank-2 Collectables Club Account. Based on that information, I learned that the Victim's computer network became infected with "Cryptowall," a particular type of ransomware, when one of the Victim's employees, using a company computer, clicked on a particular advertisement on a particular website. Once installed, the ransomware encrypted a large portion of the documents on the Victim's computer server. Along with the ransomware, a text file (.txt) appeared on the Victim's computer which stated, in sum and substance, that the Victim's files had been encrypted (i.e., rendered inaccessible) and which referred the Victim to other computer sites for instructions. The instructions on those sites directed the Victim to pay ransom, in the form of one Bitcoin, in order to obtain decryption software that would render the Victim's computer network accessible again, and provided a list of websites - including Coin.mx - where the Victim could purchase the Bitcoin. Following the instructions, the Victim's Representative contacted Coin.mx and engaged in online chats with different Coin.mx employees. When the Victim's Representative explained to one Coin.mx employee that "I'm just trying to pay the stupid cryptowall ransomware," the employee replied, "Ok please don't say anymore [*sic*] about that because then we cannot help you." Instead, the Coin.mx employee instructed the Victim's Representative to send a certain dollar amount and one cent (i.e., $xxx.01) to the Bank-2 Collectables Club account, as payment for one Bitcoin to be provided by Coin.mx.

26. From reviewing communications from Coin.mx employees to ANTHONY MURGIO, the defendant, which were recovered from MURGIO's Email Account, I learned that MURGIO and Coin.mx knowingly processed payments from ransomware victims from at least in or about April 2014, through at least in or about June 2014. However, as set forth above, based on my review of a particular Treasury Department database in or about July 2015, I learned that at no time did ANTHONY MURGIO, the defendant, or anyone else on behalf of Coin.mx, file a SAR regarding Coin.mx's participation in this unlawful activity, as they were otherwise required to do by federal law.

MURGIO'S ACQUISITION OF A FEDERAL CREDIT UNION IN FURTHERANCE OF THE UNLAWFUL SCHEME

27. As further discussed below, based on certain emails in MURGIO's Email Account, and information obtained from the National Credit Union Administration, I learned that in or about late 2014, ANTHONY R. MURGIO, the defendant, obtained beneficial control of the Credit Union, a small credit union in New Jersey with primarily low-income members, in order to process Automated Clearing House ("ACH") transactions (i.e., electronic credit and debit transactions) for the unlawful Coin.mx scheme, among other things. To do so, among other things, MURGIO made a payment to a senior executive at the credit union (the "Executive"), as reflected in bank records which I have reviewed, and also installed certain individuals close to him, including CC-1, on the Credit Union's board of directors. Below, except as otherwise noted, are relevant portions of some of the relevant communications from MURGIO'S Email Account:

a. In or about mid-2014, MURGIO engaged in numerous emails and chats with certain other individuals about acquiring a small credit union through which he could operate his Bitcoin exchange business. On or about May 9, 2014, MURGIO sent an email to CC-1 in which MURGIO described the Credit Union as "a small credit union 107 members no full time employees," and further noted that he met with Credit Union representatives and "came to an agreement that we would be able to have control of the credit union." MURGIO then invited CC-1 to become an advisory member on the board, for which CC-1 would be paid $5,000. CC-1 responded, "I am most definitely in!" and "I won't disappoint you[.]"

b. Thereafter, as reflected in numerous emails and chats in the MURGIO Email Account, MURGIO and CC-1 began to process ACH transactions for Coin.mx through a payment processor

(the "Payment Processor") which, with MURGIO's assistance, opened an account at the Credit Union, and used that account to process ACH transactions for Coin.mx and other purported businesses.

c. In October 2014, in a conversation which MURGIO recorded (a copy of which was maintained in an electronic file-storage account connected to the MURGIO Email Account, and which I reviewed pursuant to a judicially authorized search warrant), the Executive privately admitted to MURGIO that notwithstanding the Executive's titular role, "I'm going to say it. . .it's your credit union. . . I believe how I've operated from day one is it's your credit union." The Executive further worried about the "tap dancing" he and others were doing to avoid raising concern among federal regulators about the payment processing activity that MURGIO and others were conducting through the Credit Union. As the Executive further admitted, "We can't certify that all the people we let [pass] money through this credit union. . . weren't doing something illegally with the money." The Executive further acknowledged, in sum and substance, that with respect to such payment processing activity, the Credit Union had not performed appropriate Bank Secrecy Act procedures [i.e., procedures that are required under federal law and designed in part to enable law enforcement to detect money laundering and other unlawful activity by bank customers], and as a result, the Credit Union's account may have been used in furtherance of money laundering and other crimes.

28. From speaking with representatives of the National Credit Union Association ("NCUA") and reviewing NCUA records, I learned that while the Credit Union normally handled the modest banking needs of a small group of primarily low-income local residents, and had little or no experience with the business of ACH processing, by October 2014, the Payment Processor was processing over $30 million a month in ACH transactions through its account at the Credit Union. The NCUA learned of the unusual size and scope of the activity and, in part because the Credit Union did not have the AML policies or procedures in place to handle such voluminous payment processing, forced the Credit Union to stop allowing such processing; the NCUA separately required the Credit Union to remove the new Board members. Thereafter, based on emails in the MURGIO Email Account which I have reviewed, MURGIO found other ways to

process payments for his unlawful Coin.mx business, including through an overseas payment processor.

WHEREFORE, deponent prays that an arrest warrant be issued for the above-named defendant, and that he be imprisoned or bailed, as the case may be.

JOEL DECAPUA
Special Agent
Federal Bureau of Investigation

Sworn to before me this
17th day of July, 2015

HONORABLE RONALD L. ELLIS
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK